DIGITAL SELF-ERASURE OF KEY COPY-PROTECTED STORAGE

The invention is related to the field of copy protection of digital content.

Digital storage modules are increasingly being used for storing digital content such as video, music and pictures. In many applications, such as MP3 (MPEG audio layer 3) players and PVRs (Personal Video Recorders), it is essential that the content be downloaded and stored in a storage module of the local device. Content providers are allowing paying subscribers to download content that is protected by copy right. The subscribers have no right to further distribute the content, but illegal copying has become so epidemic that it is discouraging providers from providing content for subscriber download.

Content providers are looking for ways to prevent pirates from illegally distributing the downloaded content. Previously proposals to prevent illegal copying of downloaded content have not been satisfactory. Most proposals have depended on encryption of the downloaded material, but even technically unsophisticated copiers have been able to circumvent such protections. For example, A hard disc drive module used in a PVR can be removed and the encrypted contents duplicated.

In the invention herein, a storage module is provided with multiple portions of memory including a first portion and a second portion. Content is stored in the first portion and information is stored in the second portion that is required in order to access the content stored in the first portion. When unauthorized use of the storage module is detected then the second portion is blank erased so the content can not be used.

Blank erasing data is destroying data by, for example, overwriting the data with blanks, so that the data can not be recovered. Normally when data in a storage module is

erased the data itself is not modified, but a flag is marked to indicate that the location of the data is free for writing data into. One of the advantages of only blank erasing the second portion and not the first portion is that normal memory management can be used for the first portion and the special blank erasing procedure only has to be available for the second portion. Another advantage is that blank erasing may take much longer than marking that the memory position is available.

For example, the unauthorized use may be removal of the storage module from the device containing the storage module such as a VCR or MP3 player; the unauthorized use may be breaking open of the device or the module; the unauthorized use may be an attempt to read data from the module while the module is disconnected from the device.

Additional aspects and advantages of the invention will become readily apparent to those skilled in the art from the detailed description below with reference to the following drawings.

Figure 1 is a flow diagram of the method of the invention.

Figure 2 is a schematic of the system of the invention including a playing device and the connected module.

Figure 1 illustrates a flow chart of an example of the method of the invention. In step 102, multiple portions of memory are provided in a storage module. The portions of memory include a first portion for containing content and a second portion containing information that must be accessed in order to access the content stored in the first portion. In step 104, unauthorized use of the storage module is detected. The detection can include detecting: disconnection of the module from a portion of a device to which the module is connected, opening of the module, opening of the device, or attempting to access the

information stored in the module while the module is not connected to an authorized device.

The digital storage module may be, for example, a hard disc drive module or a non-volatile memory module, such as a flash card.

In step 106, access to the information in the second portion after the unauthorized use is detected is prevented. Access can be prevented for example by blank erasing a private key stored in the second section that is required for decrypting the content stored in the first section. Access could also be prevented by blank erasing a table of contents of the first portion of memory that is stored in the second portion of memory.

In step 108 a power source is provided for the detecting and preventing of access, the access also being prevented if the power source fails. Commonly a battery would be used for such a power source, and the battery could be interconnected such that when the battery died then access would be prevented.

Figure 2 is a schematic of the system of the invention including a playing device and the connected storage module. The storage module contains multiple portions of memory including a first portion (122) and a second portion (124). The storage module also contains a processors 126 containing programming modules to operate the module. The programming modules include an access control module 128 for preventing access to content stored in the first portion of memory without accessing information stored if the second portion of memory. The module contains detecting apparatus 130 for detecting unauthorized use of the storage module.

The processor also contains a protection module 132 for preventing further access of the information stored in the first portion of the memory after unauthorized use is detected. The protection module may simply blank erase the contents of the second module

whenever unauthorized use is detected. A power source 134 is provided in the module for operating the detecting apparatus and processor containing the protecting module. The protecting module preventing further access to the information stored in the first portion of the memory after the power source fails.

The unauthorized use of the storage module may include unauthorized disconnection of the storage module from a device that uses the storage module. In that case, the protecting apparatus 130 monitors the continuity of the connection 136 between the module and a portion 138 of the playing device. Whenever disconnection is detected then the protecting module 132 blank erases the second portion of the memory.

The unauthorized use of the storage module may include unauthorized opening of an enclosure 140 of the storage module. In that case, the protecting apparatus 130 monitors the integrity of the module enclosure. For example, an opening detector 152 can be connected between portions of the module enclosure and if the portions of the module enclosure are separated then opening will be detected. Whenever unauthorized opening of the module enclosure is detected then the protecting module 132 blank erases the second portion of the memory.

The unauthorized use of the storage module may include unauthorized opening of an enclosure 142 of the playing device. In that case, the protecting apparatus 130 monitors the integrity of the playing device enclosure. For example, an opening detector 154 can be connected between portions of the device enclosure and if the portions of the device enclosure are separated then opening will be detected. Whenever unauthorized opening of the device enclosure is detected then the protecting module 132 blank erases the second portion of the memory.

The information stored in the second portion that has to be accessed in order to access the contents may include a private key 144 that must be used to decrypt the content stored in the first portion of the memory in order to access the content. The storage module may contain a data decryption module 146 of processor 126 for using the private key stored in the second portion of the memory for decrypting data that is stored in the first portion of the memory. Alternately or in addition to the private key, the information stored in the second portion of the memory may include a table of contents that is necessary to play the content stored in the first portion of the memory.

The invention has been described above in relation to specific example embodiments. Those skilled in the art will know how to modify these example embodiments within the scope of the invention herein. The invention is only limited by the following claims.